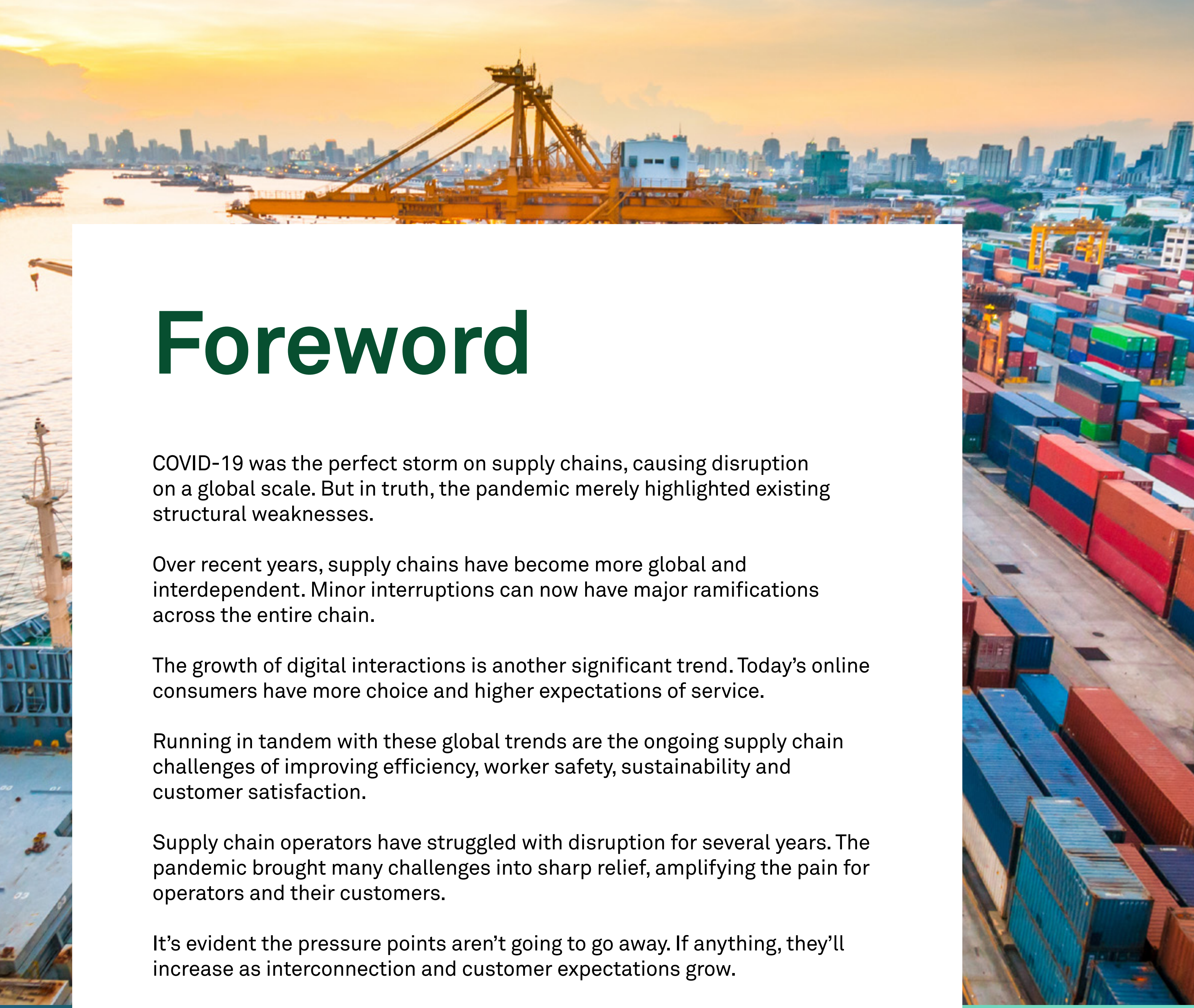
Industry Insights.

Building resilient supply chains.

Contents



Foreword

COVID-19 was the perfect storm on supply chains, causing disruption on a global scale. But in truth, the pandemic merely highlighted existing structural weaknesses.

Over recent years, supply chains have become more global and interdependent. Minor interruptions can now have major ramifications across the entire chain.

The growth of digital interactions is another significant trend. Today's online consumers have more choice and higher expectations of service.

Running in tandem with these global trends are the ongoing supply chain challenges of improving efficiency, worker safety, sustainability and customer satisfaction.

Supply chain operators have struggled with disruption for several years. The pandemic brought many challenges into sharp relief, amplifying the pain for operators and their customers.

It's evident the pressure points aren't going to go away. If anything, they'll increase as interconnection and customer expectations grow.

For many organisations, a reliable, efficient, and effective supply chain is at the core of business performance and profitability. Any inherent weaknesses must be addressed, and the organisations that proactively do so are the ones that will flourish.

While digital technologies are empowering consumers, they're also helping supply chain operators respond to growing challenges. Visibility is the overarching benefit of supply chain digitisation, which in turn can improve efficiency, sustainability and worker safety.

However, no digitisation program can afford to ignore the threat of cyber-crime.

Jon Young Flores
Industry Executive & Group Owner
Agribusiness, Supply Chain and Retail

Cyber-security

A successful cyber-attack on one of the largest logistics companies in Australia in 2019 emphasised the interdependence of supply chains. And how an attack can have widespread effects up and down the chain.

Interdependence will only increase as suppliers work more closely with each other and with their customers via communications technology and data.

Although key enablers of efficiency, both technology and data create broader attack surfaces. Cyber-criminals will exploit them because the interconnected nature of supply chain presents an irresistible target. One breach can open the door to the next.

Hackers know they can get their hands on data across multiple organisations, as well as personal customer information. Ransom demands have more chance of success because many different entities depend on the smooth running of supply.

We're also seeing the democratisation of cyber-crime, where any would-be hacker can buy malware on the dark web. That's in addition to sophisticated crime rings and rogue states using advanced AI and machine learning to automate brute-force attacks.

All of these cyber-threats increased during the pandemic as consumers switched to online shopping and many supply chain staff worked from home. It seems both trends will continue after normality returns, if not to the same extent.

As digital collaboration across supply chains becomes central to performance, the integrity of data and the systems that process it become more critical. Cyber-security now has to be a fundamental capability of supply chain organisations.

This reality has not been lost on the Australian Government. Many of our supply chains are now seen as essential to the nation, subject to the requirements of the *Security of Critical Infrastructure Act*.

Prepare for the inevitable

Every organisation is susceptible to attack. You must take the attitude that it will happen sooner or later. The more prepared you are, the better you can prevent a breach or recover from one.

> “
>
> **There are only two types of companies: Those that have been hacked and those that will be hacked.**
>
> Robert S. Mueller III
> Former FBI director

Being prepared means being aware. The gravity of cyber-threats must be taken seriously at all levels of the organisation, including your suppliers and partners. Above all, security must be a board-level priority.

Guard your information assets

The first step in protecting your supply chain is to identify the critical information assets that must remain confidential, retain integrity and be available.

The Telstra ‘five knows of cyber-security’ can help here. It offers a structure to:

1. Know the value of your data
2. Know where your data is located
3. Know who has access to your data
4. Know who is protecting your data
5. Know how well your data is protected.

A key advantage of the ‘five knows of cyber-security’ is that it focuses on outcomes rather than technology, allowing non-technical people to contribute to security management.

Once you’ve assessed the importance of your information assets, you can determine who can access it. Use the rule of least privilege: your people should access only the information they need to perform their job - and no more. The same rule should apply to your supply chain partners.

Discover the loopholes

Understanding your vulnerabilities is the next step. Many organisations don’t have a clear idea of critical systems and data so they can’t focus security measures where they’re needed most. In addition, many don’t have the tools and expertise to conduct comprehensive vulnerability testing.

In both cases, engaging an expert is advisable. For example, Telstra Purple can identify your critical information assets and support systems. They can also audit your security with a range of targeted reviews across IT infrastructure and personnel. Typically, we’ll conduct staff interviews, vulnerability scans, and a series of tests to evaluate security loopholes.

Crucially, we can apply the insights gained from protecting the largest networks in Australia - our own - as well as the latest threat intelligence from our global partners.

Invest in a security strategy

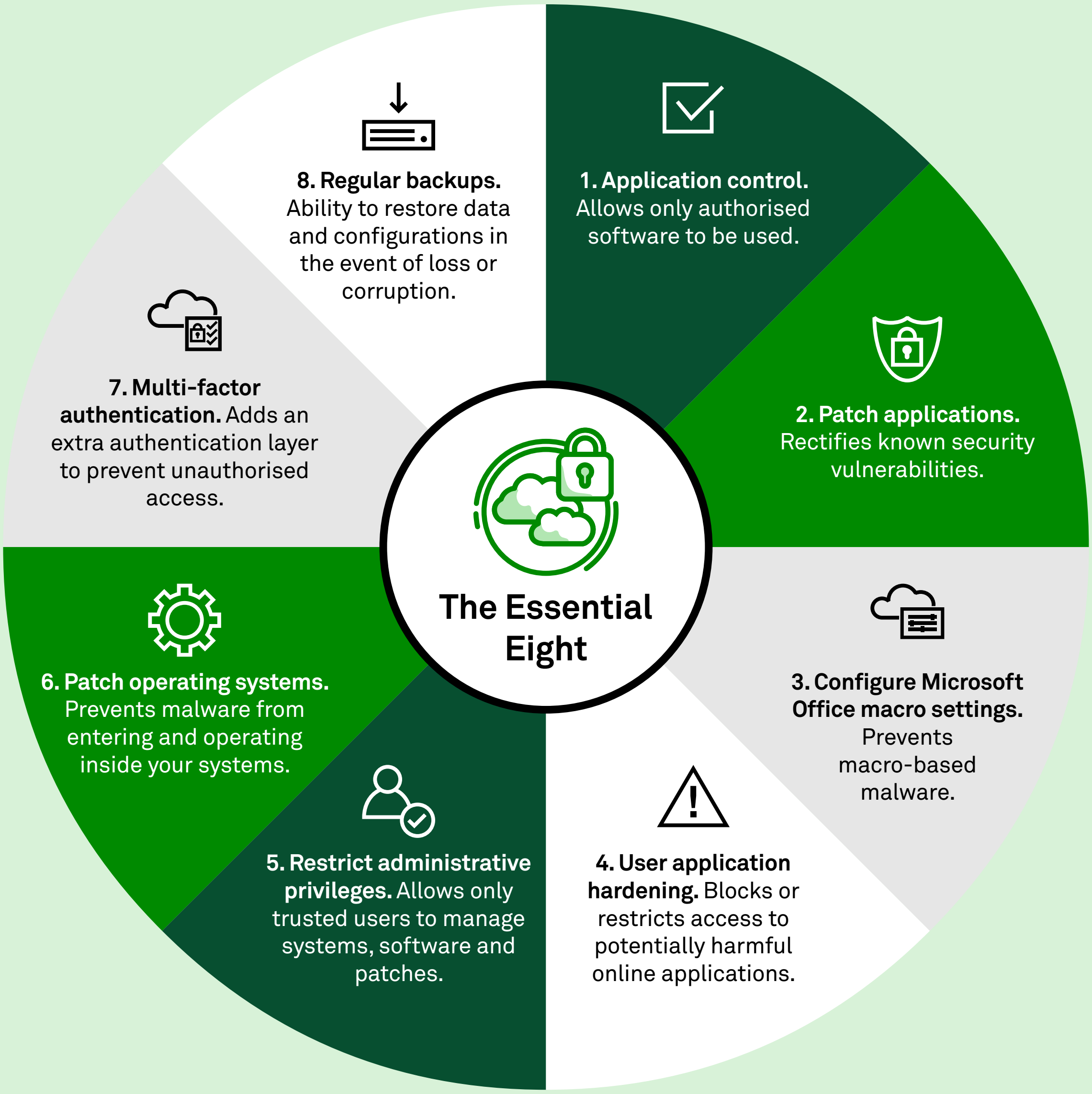
A well thought out security strategy pays dividends. However, supply chain has many moving parts and is prone to multiple and varied threats. So it’s vital to adopt a holistic strategy that covers your entire organisation as well as its partners.

What’s important is that your strategy is proactive and consistent. You don’t need large expenditure, but you do need to be good at the basics. And the best place to start is with the Australian Signals Directorate’s Essential Eight.

Apply the security essentials

The Essential Eight are the eight most essential of thirty-seven strategies identified by the Australian Signals Directorate to limit an organisation's exposure to cyber-threats. These eight strategies are easy to use, create a baseline of protection, and are a practical starting point for a strong defence.

The Essential Eight are designed to protect internet connected organisations using Microsoft Windows. While the Essential Eight can be used for cloud services, enterprise mobility and other operating systems, these are not the primary focus. The Essential Eight strategies are:



The Essential Eight

1. Application control. Allows only authorised software to be used.

2. Patch applications. Rectifies known security vulnerabilities.

3. Configure Microsoft Office macro settings. Prevents macro-based malware.

4. User application hardening. Blocks or restricts access to potentially harmful online applications.

5. Restrict administrative privileges. Allows only trusted users to manage systems, software and patches.

6. Patch operating systems. Prevents malware from entering and operating inside your systems.

7. Multi-factor authentication. Adds an extra authentication layer to prevent unauthorised access.

8. Regular backups. Ability to restore data and configurations in the event of loss or corruption.

At its most basic, the Essential Eight help you practice fundamental security hygiene. On a more strategic level, it's a shift in attitude from simply ticking security check boxes to a focus on constant vigilance and maintaining zero trust.

If you need assistance with the Essential Eight, Telstra Purple offers an Essential Eight Cyber Workshop to assess your systems and implement practices in the most relevant way.

Think ahead of the game

We can also help you go beyond the passive defence strategy of the Essential Eight through active defence initiatives. Active defence engages with cyber criminals through deception technologies.

These include honeypots and decoys to monitor criminal activities in real time to gather intelligence on their methods and objectives. Advances in automation, orchestration and virtualisation mean we can deliver honeypots and other deceptive services more affordably than ever before.

Ensure you survive an attack

A good strategy should both prevent attacks and allow you to recover quickly with minimum impact to business.

Consequently, a business continuity plan is essential. More than restoring IT infrastructure, business continuity spans all the areas of operations that need to stay up and running.

The plan should detail your response to a disruption and cover your business objectives, priorities and tolerances. It's vital to test the plan regularly to ensure it remains relevant, and allow you to improve and expand it over time.

A key advantage of planning and testing is that you can prepare for potential disruptions without the stress of an actual incident confusing your decisions.

Include your supply chain partners

Given the interdependence of current supply chains, you must assess the security posture of your partners and factor that in to your security strategy.

Perhaps the wisest course of action is to have a binding contract with your partners that defines policies and information sharing processes. It could cover risk management between you and your partners, how they store and access your data, and a plan to minimise damage if a breach occurs.

Regular risk audits should also be conducted with your partners to ensure their security posture meets the standards set out in the contract.

An ounce of prevention

There are no shortcuts to cyber-security. The reality is that a good defence requires constant vigilance and effort. Unfortunately, the only alternative is damage to your brand, financial loss and legal repercussions if a breach occurs. In this sense, good security is more than a necessity; it's a key enabler of business performance.

Operational insight

Digital technologies are revolutionising supply chains, with transformation set to continue for several years. A key advantage of digitisation is the data it generates, which can be turned into insights to support better decision-making.

Data creating devices are already commonplace to track assets, predict maintenance, gather intelligence and automate processes. They're also being used to promote safe working and reduce carbon footprint.

That's just the start. The exponential growth of IoT devices and smartphone apps will empower awareness of operations as never before, especially with the uptake of Edge computing and 5G.

Edge computing brings the cloud closer to devices in the field to process more data faster. 5G not only has better bandwidth and latency to control operations in near real time, it has the capacity to handle millions of devices at once.

The power of analytics

Advances in devices and data collection are being matched by an evolution in analytics. Until recently, there were three types of analytics:

1. Descriptive analytics to identify patterns in historical data
2. Predictive analytics to help foresee trends and possible outcomes
3. Prescriptive analytics, combining descriptive and predictive analytics, to propose actions to achieve desired aims.

Now the fourth and most exciting development - cognitive analytics - has come into play. A cognitive engine can sift through vast amounts of data in a fraction of the time compared to humans, then form conclusions on its own.

The data-driven supply chain is here

Data is adding a new dimension to supply chain management. Organisations can harvest insights from every link in the chain, from each production stage, through to sales, transport and customer fulfilment.

They'll be able to know the location and condition of goods throughout the chain, how efficient their assets and processes are, and how to improve. Greater efficiency can reduce carbon emissions, minimise shrinkage and wastage, cut costs and enhance customer service.

That's an attractive proposition to organisations dealing with environmentally aware consumers and investors who have an abundance of choice and a minimum of patience.

It's no wonder that supply chain operators are taking digitisation seriously. Many are already investing in eCommerce capabilities, site automation, tracking and monitoring devices, and digital inventory management. All of these initiatives are producing masses of data.

However, data is useless unless you extract value from it. And that presents significant challenges.

Data challenges for the organisation

Where data analytics was once the privilege of larger organisations, the cloud has brought data storage and analysis within reach of all. Massive computing power coupled with proven tools and algorithms are now available without major investment.

However, evaluating data within the business context is essential to deliver value. It requires data scientists to extract meaning relevant to the specific needs of the business.

Analytics expertise like this is in short supply, with demand constantly growing. Even larger organisations may need to source expertise from data specialists like Telstra Purple, who can analyse business goals and create rules to differentiate between critical and non-critical data.

Once the business rules are defined, data needs to be collected in a timely fashion, be accurate, and be processed in a repeatable manner.

Data challenges across the industry

The supply chain industry, in common with other Australian industries, faces several hurdles when committing to a data-driven future.

Supply chain organisations are frustrated by the difficulty of accessing scarce skills to deploy digital technologies. Many are also unwilling to move their entire operation over to a data-driven model since it is such a complex process.

Security is a major challenge. Data needs to be secured in storage and in flight to prevent breaches and the resulting fallout. Good security hygiene is a must, especially when sharing data among different organisations. As noted previously, one breach can have impacts up and down the chain.

Data sovereignty can also be an issue. Digitisation creates masses of data which will most likely be stored in the cloud. Many organisations don't want their data stored offshore under foreign privacy regulations. Luckily, Telstra stores all data in Australia, subject only to Australian law.

Data sharing is a concern. Although many see the value of data collaboration outside the organisation, others are still wary of giving away critical information, and by inference, competitive advantage. However, new data sharing platforms let you control what you share, with whom, and for what purpose. There's little risk and much to gain.

Data quality and accuracy is another significant problem. Goods and assets are often tracked using different systems so data has to be translated into the correct format when it is shared. Worse still, some information is not on digital systems because of paper-based processes.

The lack of consistent data standards presents the same problem on a national scale. At present, the cost and time of standardising data when aggregating it for analysis is a major obstacle to progress.

At Telstra, we believe a national data standard for supply chain developed by industry players and governing bodies is a matter of urgency. Other countries already have it, and we need to emulate them to stay competitive - for our businesses, industries, and as a nation.

Telstra is applying lessons learned

Telstra operates and is reliant on several sophisticated supply chains. These service our widespread retail operations, support our enterprise customers and the ongoing development and maintenance of the most extensive and critical network and IT infrastructure in the country.

When we provide services, products and technologies to help our customers digitise and secure their supply chains, we draw on this vast experience. It enables us to take a proven, pragmatic, and results focused approach.

We also benefit from being a technology company. We understand where technology is heading, and have partnerships with global tech companies to develop new and innovative solutions.

Many of these innovations are already benefiting our customers:

- **Telstra Track and Monitor:** Centralised tracking of moving assets on and off site to cut costs and improve efficiency
- **Connected Vehicles:** Improve visibility, safety and productivity across your people and vehicles.
- **Visibility Imports:** Locate, track and identify ocean freight in transit regardless of shipping line or freight forwarder, enabling you to take corrective action and optimise operations.

And lastly, there are our networks that have been connecting people and businesses decades. We own the largest and most advanced networks in Australia, including the largest IoT network covering almost 50% of the country.

Leveraging these strengths, we are developing solutions both for ourselves and our customers, and can recommend practical strategies to transform supply chains.

Avoid a complete transformation

The cost, complexity and time to value of digitising your supply chain are daunting, especially if you're looking at your entire operation. We think transforming everything at once is not only impractical, it can be counter-productive in an evolving industry where needs may change over time.

Instead, we favour a step-by-step method. Start with the basics, focus on immediate results, then build incrementally over time. Plan where you want to be year by year and adjust as you go.

That's the approach we've taken for our own supply chain, and we believe it will deliver for our customers too. All of the solutions we're developing revolve around four key principles. They must:

1. Work straight out of the box
2. Be modular and scalable
3. Be digitally native
4. Deliver tangible results from day one.

Importantly, we're developing solutions for each industry, since each is unique. In this way we can address industry-specific issues while delivering the economies of scale and time to value that's impossible with custom solutions. Being modular, the solutions offer the flexibility to start small and build up as needed.

Embrace data sharing

While many have reservations about sharing data, we believe this is a key advantage of digitisation. In fact, seamless data collaboration delivering powerful insights is one of the most important ways to drive productivity and innovation.

Obviously, security and robust data sharing agreements have to be in place before data is shared. It also helps if organisations sharing data have aligned goals to gain mutual benefits. Nevertheless, the rewards are definitely worth the effort.

Because data sharing is so important, we've developed the Telstra Data Hub. This cloud platform enables participants to share data and insights inside and outside their organisations securely, at scale, and with control.

Participants choose who they share data with at an individual or organisational level. They can view and set rules and select licence types for the level and type of usage. In effect, data contributors have complete, granular control of what they share.

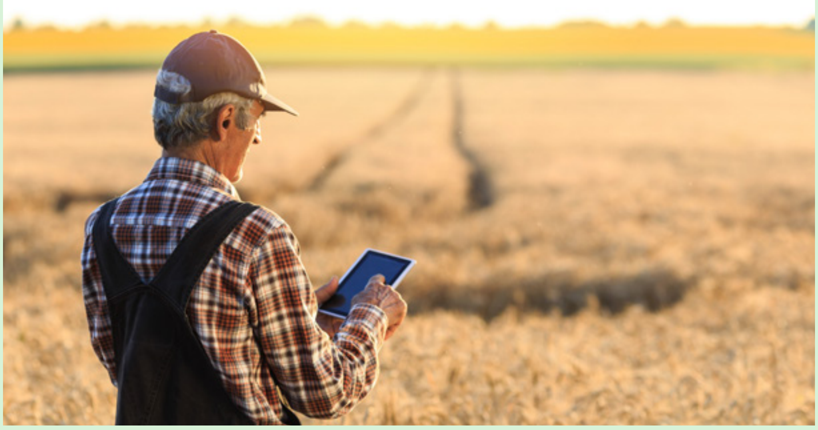
Meanwhile data consumers can tap into a wealth of information across businesses, industries, governments, IoT sensors, satellites, weather information and more to create deeper insights.

A unique feature is the ability to acquire specific data segments, not the entire data set, to reduce the time and cost of analysis.

To address the problem of conflicting data standards, the Telstra Data Hub automates the processes of data integrity, technology integration, security and provenance at an industry level. This makes data analysis and sharing secure, simple and fast.

Safe, effective data sharing

Telstra developed a pilot for a ‘hyper-local’ weather data and forecast system for the Bureau of Meteorology. Once data is collected, checked, cleaned, and organised by the Telstra Data Hub, it will be used to deliver previously unobtainable weather insights. Forecasts and observation data can be confidently shared by project participants since the Telstra Data Hub’s management system helps protect private information and support private data suppliers’ interests.



We’re testing a hyper-local weather network for Australia’s farmers.

Read more >

Get a better view of workplace safety

No assessment of digitisation would be complete without exploring its role in workplace safety.

Safety is already a priority in the industry. Employers know they have a legal and moral obligation to ensure the wellbeing of employees and the public. Chain of Responsibility legislation means customers also have a role to play.

Now, digitised operational visibility provides new and more effective ways to keep both people and plant safe.

For example, video analytics can use AI to identify conditions and emerging behaviours that might lead to incidents before they occur, then recommend interventions. More specifically, video analytics (including facial recognition) can monitor driver behaviour, detect when a driver is drowsy or not concentrating, and alert the driver.

Vehicle tracking/monitoring can help ensure vehicles are operating at optimum efficiency, and that drivers are not pushing vehicles beyond their limits. This not only keeps drivers safe, it can reduce wear and tear on vehicles.

In addition, personal tracking devices can monitor the condition and location of remote or lone workers, and allow them to alert the organisation if they are under duress or need help.

The near future

Several new technology developments hold immense potential to transform supply chain management. Telstra is investing in three of the most important:

1. Cognitive analytics engines

Cognitive engines use AI, Machine Learning and sophisticated algorithms to analyse structured and unstructured data. A cognitive engine can reason, learn, and even interact in human language. It can then form conclusions and propose actions from those conclusions. And since the engine learns on the job, it can fine-tune the accuracy of conclusions over time.

Technology companies across the globe are developing this capability, including Telstra. In fact, Telstra's Cognitive Control Tower is already monitoring weather data to predict networks outages and formulate responses with minimum human intervention. It's performing well beyond expectations and soon this solution will be available to our customers.

2. Digital Twins

A Digital Twin is a digital model of a physical asset, whether a factory floor, an entire city system, or a supply chain. You can make changes to the digital model to predict scenarios and outcomes without the time, cost and disruptions of the physical world.

For example, you could create a digital version of your supply chain and do modelling to see if it could be more efficient. Or you could stress-test it to discover possible bottlenecks and disruptions if specific events occurred.

Multiple scenarios could be run to understand different impacts from different events, evaluate the most effective responses, and prepare ahead of time.

Telstra has already developed an office Digital Twin across five of our commercial buildings. In addition, we're leading a consortium to develop a proof-of-concept Digital Twin for the state of New South Wales. This will assist the government respond to disasters, including wildfires.

3. Distributed ledgers, blockchain and smart contracts

A distributed ledger is a digital database across multiple parties and locations. Unlike centralised databases, a distributed ledger does not have a central point of authority to verify transactions. Instead, transactions are verified by all parties in the ledger.

Decentralised verification avoids the single point of failure or corruption that can occur with a centralised database. In addition, transactions are time-stamped and have cryptographic signatures. All this means that transactions should be tamper-proof and auditable.

Blockchain is a type of distributed ledger where each transaction in the chain depends on the preceding transaction, and the entire sequence requires proof of work at every step.

Other distributed ledgers do not depend on a chain of transactions or proof of work, making them simpler to operate and scale.

Smart contracts are a key aspect of distributed ledgers. Smart contracts are computer-based protocols that manage transactions between buyer and seller according to the terms of their contract. Since the contract terms are contained in the computer code itself, transactions are fully automated.

Automation, accuracy and authentication are the key advantages of these technologies. This offers significant benefits to supply chain operators.

Firstly, they can connect different aspects of the supply chain like inventory, communications and financials, creating a single source of truth to improve decision-making.

Secondly, the technologies can support more accurate tracking of goods, reduce errors and provide more effective proof of provenance.

And finally, they can dramatically cut the cost and time of managing transactions across multiple participants in the chain.

All of which fits the key supply chain aims of driving visibility, efficiency and economy across complex and distributed supply chains.

Conclusion

Although the pandemic exposed and aggravated critical weaknesses in supply chain, it's evident that technology and data can go a long way to addressing them. Digital initiatives can form the foundation of a connected, resilient supply chain that is essential not just for survival in a dynamic and hyper-competitive global economy, but for driving business advantage.

In the not too distant future, technology and data have the potential to totally transform supply chains, enabling management to be more responsive, predictive and accurate. The resulting advantages will touch every aspect of supply chain to drive increased efficiency, enable improved customer experiences and worker safety, and help businesses operate more sustainably.

Forward-thinking organisations willing to adopt these new digital capabilities are the ones that will get the edge. Telstra is standing by to help with a precise, step-by-step approach that can deliver measurable results with less risk, complexity and cost than thought possible.

How Telstra can help

Security Consulting

purple.telstra.com/services/cyber-security

Telstra Purple was named Leader in the 2021 ISG Provider Lens Quadrant for Technical Security Services. Our security team can assist you with all aspects of cyber-security including:

- Governance - what to do
- Risk - why it needs to be done
- Solutions - how it is done?
- Assurance - is it done?

Security Management

telstra.com.au/business-enterprise/products/security

- **Business Security:** A range of managed services to ensured security, governance, privacy and compliance.
- **Cloud Security:** Advanced cloud delivered security services to speed cloud adoption while maintaining flexibility and performance.
- **Workplace Security:** Proven technologies backed by managed services to protect distributed workplaces and workers.

Telstra Data Hub

telstra.com.au/business-enterprise/products/internet-of-things/solutions/telstra-data-hub

A secure data collaboration platform to support deeper insights and more accurate decisions.

Connected Supply Chain

telstra.com.au/business-enterprise/industries/supply-chain

- **Telstra Track and Monitor:** Automated, mapped tracking to manage moving assets more efficiently and economically.
- **Connected Vehicles:** Fleet management and collision avoidance solutions to improve productivity, efficiency and safety.
- **Visibility Imports:** A single view of ocean freight tracking and reporting, regardless of shipping line or freight forwarder.

Internet of Things

telstra.com.au/business-enterprise/about-enterprise/our-network/iot-coverage-map

- **Connectivity:** Telstra has Australia's largest IoT network with technologies including Cat M1, NB-IoT and 4G/5G.
- **IoT Capabilities:** We offer end-to-end capabilities, from devices, local and global connectivity, to management platforms and professional services.
- **IoT Solutions:** A range of complete IoT solutions to monitor, manage and protect everything from fixed and movable assets to entire environments.

Contact your Telstra account representative for more details.

☎ **1300 telstra** (1300 835 787) **telstra.com.au**